ware components from said software-loading-system into said computer system according to said list, to create a predetermined software configuration on said computer system; wherein said configurations and database structures are secure from alteration by other than authorized users and processes.

According to another disclosed class of innovative embodiments, there is provided: a process for controlling manufacture of computer systems by a contract manufacturer, comprising the steps of repeatedly: assembling hardware components into a predetermined hardware configuration, to create a computer system; connecting said computer system to a computer network with a software-loading-system, said software-loading-system being a secure computer system which is protected against any undetectable alteration by said manufacturer and comprising a server containing software installation configurations and a database structure which manages said configurations; selectively downloading software components from said software-loading-system into said computer system, to create a predetermined software configuration on said computer system; maintaining a database which shows the component configuration created by said steps (a.) and (b.), on each computer system; said database being protected against any undetectable alteration by said manufacturer; and repeating said steps (a.) through (d.), to manufacture computers with varying configurations.

Modifications and Variations

As will be recognized by those skilled in the art, the innovative concepts described in the present application can be modified and varied over a tremendous range of applications, and accordingly the scope of patented subject matter is not limited by any of the specific exemplary teachings given.

Splitting the databases between two different servers can be used as an approach to regulating the resources used by any a given server at the remote manufacturing facility. A spilt-server architecture is possible without the expense of a second network.

Database security can be increased to afford tighter control over data or loosened to allow remote manufacturers greater access to the data.

Firewalls or other network security devices can be used within the remote manufacturing facility to prevent access to data held in master databases at the facility.

The MD5 check value is merely one way of efficiently checking a file's contents for corruption. Other values or hashing functions can be substituted for the MD5 value in order to confirm the file has reached the remote manufacturing facility line servers unaltered.

The as-built database tracks third-party hardware and software but could be narrowed to track only that software produced and installed by the manufacturer.

In the alternative embodiment, the network topologies and bandwidths described above are not the only bandwidths which can be used. In fact, different network topologies may demand higher or lower bandwidths. For example, the FDDI standard provides for a much higher bandwidth while Appletalk is much more narrow.

What is claimed is:

1. A system of software pre-installation, comprising:

(a.) a computer network with one or more servers containing software installation configurations, a first database structure which manages said configurations, and a second database structure which manages component selection rules;

(b.) at least one assembled unit connected to the network and in communication with said server;

(c.) a component configuration process which accesses said second structure to produce a list of hardware and software as it is installed on said assembled unit; and

(d.) a software pre-installation process which accesses said database structures and said software installation configurations to automatically pre-install software onto said assembled unit;

wherein a contractor has physical access to said servers, but said configurations and database structures are secure from alteration by other than authorized users and processes.

2. The system of claim **1**, wherein one database structure contains the information of said first and said second database structures.

3. The system of claim **1**, wherein said first database structure and said second database structure exist on separate servers.

4. The system of claim **1**, wherein said first database structure and said second database structure exist on separate servers and said separate servers are connected to different networks of varying bandwidths.

5. The system of claim **1**, wherein said first database structure exists on server connected to a higher bandwidth network than said second database structure.

6. The system of claim **1**, wherein said list is used to store as-built information for each said assembled unit.

7. A system of software pre-installation, comprising:

(a.) a computer network with a first server containing software installation configurations and a first database structure which manages said configurations;

(b.) a second server containing a database structure which manages component selection rules;

(c.) at least one assembled unit connected to the network and in communication with said servers;

(d.) a component configuration process which accesses said second server to produce a list of hardware and software as it is installed on said assembled unit; and

(e.) a software pre-installation process which accesses said list, said first database structure, and said software installation configurations to automatically pre-install software onto said assembled unit;

wherein wherein said configurations and database structures are secure from alteration by a software installer said first server has a higher bandwidth than said second server.

8. The system of claim **7**, wherein said first database structure access said list to automatically download said software.

9. The system of claim **7**, wherein said wherein said first database structure exists on server connected to a higher bandwidth network than said second database structure configurations and database structures are secure from alteration by other than authorized users and processes.

10. The system of claim **7**, wherein said list is used to store as-built information for each said assembled unit.

11. A system of software downloading, comprising:

(a.) a computer system comprised of hardware components assembled into a predetermined hardware configuration;

(b.) a computer network comprising a software-loading-system, said software-loading-system being a secure computer system which is protected against any undetectable alteration by a manufacturer and comprising a